UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/464,854	12/16/1999	BRUCE ARLAND RICH	AUS990150US1	8177

7590 06/30/2004

DAVID H JUDSON
HUGHES & LUCE LLP
1717 MAIN STREET
SUITE 2800
DALLAS, TX 75201

EXAMINER	
GURSHMAN, GRIGORY	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 06/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/464,854	RICH ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The formal drawings filed on 3/08/04 are accepted by examiner.

Response to Arguments

2. The rejections of claims 1,9,14,15 and 18 under 35 USC § 112 are withdrawn in view of the Applicant's amendments of the instant claims.

3. Applicant's amendment of the independent claims 1, 9, 14, 15, 18, 22 reflect " the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation". This limitation is taught by O'Toole. Adding the access ticket to the access control list of the channel object of the client computer (see Fig.1 and Fig. 2, block 30) meets the "security modification" being "a predetermined event". Examiner points out that modifications of access control list constitute "an attempt to circumvent a security mechanism of the trusted computer installation".

4. Applicant's amendments of the dependent claims are addressed in the rejections herein.

5. Referring to claims 1-23, Applicant argues that O'Toole does not teach some of the features claimed by Applicant. In particular, Applicant point out that O'Toole does not teach determining that a user has made a security modification to the trusted computer installation. Examiner points out that using broad but reasonable interpretation, one of ordinary skill in the art would have equated a security modification with adding the

access ticket to the access control list of the computer. Further more, O'Toole teaches a "notification event" in a form of sending the access ticket to the notification server. Examiner also points out that the addition of a new access ticket to the access control list is a circumvention of the security mechanism as this action can potentially allow an unauthorized user to access the trusted compute installation. Therefore, examiner maintains his position that O'Toole anticipates and obviates the instant claims respectively.

6. Referring to claims 9 -11, 13, 14, 15 – 21, Applicant argues that neither O'Toole nor IBMC, alone or in combination teach instantiating a security manager class. Examiner respectfully disagrees and points out that IBMC teaches that the settings for each of the operation checks are defined by the JAVA security manager class (see page 2, basic-abstract). Examiner maintains that one of ordinary skill in the art would have been motivated to determine that a security modification has been made to the computing installation and invoke a JAVA security manager class as taught in IBMC for defining the settings of the operation to be performed (see IBMC, page 2, basic abstract). The limitation" instantiating the security manager class" is met by parameters required for the application (see abstract).

7. Referring to the instant claims, Applicant further argues that the combination of O'Toole and IBMC is based on hindsight reconstruction of Applicant's disclosure. Examiner respectfully disagrees and points out lin response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a

reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

8. Referring to claims 2 and 12, Applicant's arguments are primarily based on the same reasons as in claims 1 and 9. Referring to the instant claims examiner maintains the same position.

9. Rejection of claims 1-23 are maintained.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1, 4 - 6, 8, 22 and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by O'Toole (U.S. Patent No. 6.279.112 B1).

12. Referring to the instant claims, O'Toole discloses control transfer of information in computer networks (see abstract and Fig.1).

O'Toole teaches that the client computer notifies the server computer (or the information source computer) that the access ticket was added to the access control list - see column 5, lines 23-30 and Fig 2, block 32. O'Toole teaches that client computer 200 also stores a client security profile 208 that specifies that certain information in client personal profile 206 should be disclosed to server computer 202 only to trusted servers or only upon authorization from the client user or both. A client "avatar" 210 located at client computer 200 acts as an agent for the user by controlling the release of information from client personal profile 206 to server computer 202 (see Fig.5).

13. Referring to claim 1, the limitation "determining that a user has made a security modification to a portion of the trusted computing installation" is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig.1 and Fig. 2, block 30). The limitation "determining that the security modification is a notification event if the security modification is a predetermined event indicative of an attempt to circumvent a security mechanism of the trusted computing installation" is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig.1 and Fig. 2, block 30) and by sending the access ticket to notification server (see Fig. 2, block 30). The limitation "sending the central authority a notification of the security modification in response to determining that the security modification is a notification event " is met by client computer notifying server computer that access ticket was added to access control list (see Fig. 2, block 32), which constitutes the security modification.

14. Referring to claim 4, O'Toole teaches addition of the ticket to access control list, which can allow a number of events to be modified by a user upon authorization.

15. Referring to claim 22, the limitation "a pluggable framework for receiving a set of notification objects..." is met by notification server (see block 16 in Fig. 2).

16. Referring to claims 5 and 6, it is inherent to send notifications in the form of Simple Network Management Protocol (SNMP) alerts or in the form of an e-mail messages or screen messages.

17. Referring to claim 8, it is inherent to use the Java Virtual Machine on the client for using Java Applets verifications.

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 9 -11, 13, 14, 15 - 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Toole (U.S. Patent No. 6.279.112 B1) in view of INT BUSINESS MACHINE CORP (RD 414099A).

20. Referring to the instant claims, O'Toole discloses control transfer of information in computer networks (see abstract and Fig.1). O'Toole teaches that the client computer notifies the server computer (or the information source computer) that the access ticket

was added to the access control list - see column 5, lines 23-30 and Fig 2 , block 32. O'Toole teaches that client computer 200 also stores a client security profile 208 that specifies that certain information in client personal profile 206 should be disclosed to server computer 202 only to trusted servers or only upon authorization from the client user or both. The limitation "determining that a user has made a security modification to a portion of the trusted computing installation" is met by adding the access ticket to the access control list of the channel object of the client computer (see Fig.1 and Fig. 2, block 30). The limitation "determining that the security modification is a notification event of interest" is met by sending the access ticket to notification server (see Fig. 2, block 30). The limitation "sending the central authority a notification of the security modification" is met by client computer notifying server computer that access ticket was added to access control list (see Fig. 2, block 32). O'Toole, however, does not teach or suggest the use of a security notification manager class.

21. Referring to the instant claims, INT BUSINESS MACHINE CORP (hereinafter IBMC) discloses a security environment for evaluating and executing Java applications (see abstract). IBMC teaches that the settings for each of the operation checks are defined by the JAVA security manager class (see page 2, basic-abstract). Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to determine that a security modification has been made to the computing installation of O'Toole and invoke a JAVA security manager class as taught in IBMC. One of ordinary skill in the art would have been motivated to determine that a security modification has been made to the computing installation and invoke a JAVA security

manager class as taught in IBMC for defining the settings of the operation to be performed (see IBMC, page 2, basic abstract). The limitation" instantiating the security manager class" is met by parameters required for the application (see abstract).

22. Referring to claims 10,16 and 23, it is notoriously well known in the art to use notifications in the form of Simple Network Management Protocol (SNMP) alerts or in the form of an e-mail messages or screen messages.

23. Referring to claims 7 and 18, the limitation "invoking an abstract Java class" is met by IBMC disclosure, teaching the use of the JAVA security manager class (see page 2, basic-abstract).

24. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over O'Toole (U.S. Patent No. 6.279.112 B1) in view of Renaud (U.S. Patent No. 5.958.051).

25. Referring to claim 2, O'Toole teaches sending the central authority a notification of the security modification made on the client computer. O'Toole teaches addition of the ticket to the access control list, which meets "addition of the certificate in a certificate database". O'Toole, however does not explicitly teach the notification in the form of applet signature. Renaud discloses implementing digital signatures for data streams (see abstract). Renaud teaches computer-implemented method for verifying the authenticity of data wherein when the data file comprises an applet, and when the signature is not verified, the method includes determining whether an unsigned data file is acceptable for execution on the computer, and terminating the applet if an unsigned data file is not acceptable for execution on said computer (see Fig. 6 and column 17,

lines 3-9). Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to send the notification of the security modification to the central authority of O'Toole in the form of failed applet signature as taught in Renaud. One of ordinary skill in the art would have been motivated to send the notification of the security modification to the central authority in the form of failed applet signature as taught in Renaud for determining whether to allow or disallow applet action (see Renaud, Fig 6, blocks 618 and 620).

26. Claims 3 and 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over O'Toole (U.S. Patent No. 6.279.112 B1) in view of INT BUSINESS MACHINE CORP (RD 414099A) and further in view of Renaud (U.S. Patent No. 5.958.051).

27. Referring to claim 12, O'Toole and IBMC teach determining that user has made a security modification to a portion of computing installation and sending the notification to the central authority. O'Toole and IBMC, however do not teach the use of applet signature verification routine for determining the security modification. Renaud teaches computer-implemented method for verifying the authenticity of data wherein when the data file comprises an applet, and when the signature is not verified, the method includes determining whether an unsigned data file is acceptable for execution on the computer, and terminating the applet if an unsigned data file is not acceptable for execution on said computer (see Fig. 6 and column 17, lines 3-9). Renaud shows applet signature verification routine (see Fig.6, block 606). Therefore, at the time the invention was made it would have been obvious to one of ordinary skill in the art to determine

that user has made a security modification to a portion of computing installation of O'Toole and IBMC by running the applet signature verification routine as taught in Renaud. One of ordinary skill in the art would have been motivated to determine that user has made a security modification to a portion of computing installation by running the applet signature verification routine as taught in Renaud for accepting the signed stream or stopping the applet (see Renaud, Fig. 6 blocks 624-625).

Conclusion

28. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (703) 306-2900. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the TC 2100 receptionist whose telephone number is (703) 305-3900.

GG

Grigory Gurshman
Examiner
Art Unit 2132

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100